exabeam

Solution Brief

Your Greatest Adversary Could Be an Insider Threat

Dealing with Malicious Insiders

According to a recent Ponemon Institute report, malicious insiders contribute to 26% of insider threats. An insider threat is malicious activity against an organization that comes from user credentials with legitimate access to an organization's network, applications, or databases. These credentials can belong to anyone with access to the organization's physical or digital assets: current employees, former employees, or third parties like partners, contractors, or temporary workers.

Insider threats are commonly divided into three categories: malicious insiders, careless insiders, and compromised insiders. Whereas careless and compromised users unknowingly threaten an organization, a malicious insider is an employee or contractor who deliberately looks to steal information or disrupt operations. A malicious insider may be an opportunist looking for ways to steal information that they can sell or which can help them in their career, or a disgruntled employee looking for ways to hurt an organization, or punish or embarrass their employer.

A malicious insider's access to and knowledge of the organization's most valuable assets makes attacks from malicious insiders harder to identify and remediate than those that originate from outside the organization. Signatures are designed for these types of adversaries, who essentially could be classified as a zero day attack because of their legitimate credential use. Organizations must trust insiders and grant them the access and resources needed to do their job effectively; this often includes access to sensitive data that can be sold or potentially used to cause harm to the organization:

1. **Financial reporting data** — early access enables illegal trading in a company's stock
2. **Customer data** — can be downloaded and sold to competitors
3. **Product or technical documents** — valuable assets that can be sold or taken to competitors
4. **Employee personally identifiable information (PII) data, and more.**

If an insider sabotages business operations or steals intellectual property or sensitive data, the financial, regulatory, and reputational repercussions can bring huge fallout; however, conventional security tools offer little detection power to distinguish whether authorized actions have malicious intent.

Exabeam for threats from malicious insiders

Detecting, investigating, and responding to threats from malicious insiders can help reduce the chance of a system compromise or a breach. In doing so, organizations can save substantial amounts of time investigating, save money resolving threats, and avoid the loss of brand reputation and customer trust associated with a breach.

As a pioneer in UEBA, Exabeam behavioral analytics is always working in the background to baseline what normal activity looks like for every user or asset in an organization. Understanding normal activity provides users a powerful defense beyond the rules and correlation found in legacy SIEM tools. Exabeam stitches together both the normal and abnormal behavior of users and machines. These timelines include all information an analyst needs to perform a rapid investigation, including: normal and abnormal behavior, as well as the surrounding context, like what happened before and after an alert, or if this alert maps to a MITRE tactic, technique, or procedure. Add to this, Exabeam responds to internal attacks from malicious insiders with packaged use case content that includes end-to-end workflows. This prepackaged content includes detection rules, models, and workflows to simplify focus on addressing these threats.

Detect data access abuse

With the proliferation of various applications to collaborate across the business, employees have gained unprecedented access to sensitive data housed in file shares, content management systems, databases, and more. Testing access to and staging sensitive data is often the first step malicious insiders take before a data leak, which can mean huge financial and reputational costs to the organization.

Traditional security tools are unable to distinguish employees accessing sensitive data for normal business purposes from data access abuse such as snooping on customer information, sensitive information like medical records, and more. Furthermore, these tools lack the ability to leverage context to identify the intent behind user activity.

With the support of automation and use case content across the full analyst workflow, from detection to response, Exabeam helps security and insider threat teams detect users abusing their access to data. Instead of forcing analysts to connect the dots across data silos, Exabeam automatically assembles alerts, activity, and contextual data, and analyzes it from the user's point of view, reducing the likelihood of missing an internal threat. Behavioral analytics develops a baseline of normal activity for every user and device, and flags anomalous behavior indicating malice in a user's risk score. Machine-created timelines allow security and insider threat teams to easily investigate event details with minimal technical expertise and without repeatedly querying multiple systems. A guided investigation checklist and automated response playbooks enable analysts to quickly and effectively remediate incidents and reduce mean time to respond (MTTR).

Recognize suspicious behavior on privileged accounts

Privileged accounts such as administrators or executives often have access to sensitive information or critical assets, making them rife for abuse. Insiders may use these privileges to enact regulatory, operational, financial, and reputational harm to an organization.

Legacy security tools struggle to integrate contextual data to identify activity associated with privileged accounts and assets. This means malicious behavior such as account manipulation or abusing service or executive accounts may go undetected.

Exabeam leverages context to create watchlists and continuously monitor privileged users and assets for changes in their risk score that may indicate suspicious activity. From a watchlist, an analyst can navigate to a user or entity timeline to gain further visibility into privilege abuse. Timelines leverage patented host-IP-user mapping to automatically aggregate security alerts, events, and a user or entity's activity — both anomalous and normal — and assemble them into clear, readable events, all without an analyst needing to write a single query. For further investigation, Exabeam provides a behavior-based threat hunting tool capable of honing in on the abnormal activity associated with privilege abuse, such as non-executive users accessing executive assets. At each step of the way, analysts can reference our privilege abuse checklist to ensure their investigation is thorough and complete.

Recognize data leaks

To support operational efficiency, data moves in and out of an organization. However, enabling access to data from outside the network perimeter introduces greater risk from malicious insiders. Easy accessibility to data provides an opportunity for malicious insiders with privileged access and knowledge of the organization's most valuable assets to exploit data. Instances of a data leak can closely resemble normal activity, making it more challenging for security teams to identify threats from insiders than threats that originate from outside the enterprise.

To reduce the risk of a data leak, Exabeam uses behavior to understand the context and risk associated with incidents. Understanding context enables organizations to recognize malicious instances of a data leak. Exabeam prescribes useful data sources such as DLP tools, email, application, and endpoints to collect and analyze. User and entity behavior analytics (UEBA) then develops a baseline of normal activity for every user and device in an organization. As an insider begins to move within a network, abnormal activity is identified using pre-packaged detection rules and models.

Painting a full picture of user activity allows analysts to leverage user and asset contextual data in conjunction with the DLP alerts to determine if the insider is acting with malicious intent.

Uncover audit tampering

Organizations increasingly rely on audit logs as a detailed record of user and system activity. Many threat detection tools analyze these logs to track user behavior, identify anomalies indicative of user compromise, or support incident investigation. However, malicious insiders aware of organizational practices may circumvent detection by clearing or tampering with audit logs. Without a reliable system of record, security and insider threat teams using traditional security tools are unable to identify or investigate these types of threats.

Exabeam provides a reliable record of user activity to help identify whether the underlying logs have been altered or deleted. Exabeam playbooks orchestrate response to audit tampering incidents. Pre-built integrations and customizable actions enable analysts to automate playbooks to respond to audit tampering, such as suspending a user or resetting a password.

Detect abnormal destruction of file data

Organizations with recent restructurings, terminations, or other major events can often leave employees disgruntled. With access to sensitive data and critical systems, these employees can wreak havoc by disrupting or halting business operations. Because file deletion is generally considered normal, permissible activity, security and insider threat teams are often unable to detect these types of threats. By the time teams are aware of an incident, the damage is already done.

Exabeam gives complete visibility into malicious insiders destroying data. Smart Timelines™ automatically capture and assemble all activity data, including events leading up to and after file deletions. Exabeam playbooks offer security and insider threat teams a guide to respond to the destruction of data. Analysts can choose to automate responses, including suspending a user or resetting a password for a user they have detected attempting to destroy file data.

At-risk employees

At-risk employees, aka "leavers," pose a significant threat to an organization as they may at any time decide to leave the organization with little to no advance notice. While most employees who decide to exit an organization will maintain their professional responsibilities through their final day, some will, unfortunately, use their last days with the organization to access, exfiltrate, or destroy critical business assets.

Early identification and monitoring of users exhibiting signs of leaving an organization will help organizations mitigate the damage insiders who aim to cause monetary, reputational, or operational harm to the organization can inflict before exiting.

Exabeam supports the detection of, investigation of, and response to an employee exhibiting signs of leaving an organization or communicating with a competitor via email, including searching for jobs or sending files to a personal email address. Exabeam leverages machine learning and user behavior analysis to automatically detect abnormal behavior that could indicate an employee is at risk of leaving the organization and taking sensitive data. By learning and understanding the expected behavior of each user and their peer group, Exabeam can distinguish any

abnormal behavior. Data Insights Models include additional details about anomalies.

Exabeam models the large volume of events to identify unusual user behaviors and alerts analysts in real time of behaviors such as a sudden user uptick in activity, uploading data to job search sites, sending sensitive data to their personal email addresses, or printing documents.

Smart Timelines™ automatically assemble and present a user's session of activities, including the lists of accounts and systems accessed, thereby eliminating tedious manual evidence gathering. Analysts can also create watchlists of suspected leavers, making it easy to monitor their behavior closely.

Exabeam Fusion

As the leading Next-gen SIEM and XDR, Exabeam Fusion provides a cloud-delivered solution for threat detection and response. Exabeam Fusion combines behavioral analytics and automation with threat-centric, use case packages focused on delivering outcomes. Exabeam Fusion is modular; we can augment your legacy data lake or SIEM deployment with XDR, or replace your SIEM entirely. It's your call.

Exabeam Fusion provides:

- Faster threat detection and response, as much as 50% faster
- Advanced alert triage capabilities — 83% of analysts report the ability to triage twice as many alerts as a legacy SIEM
- Built-in automation with predefined workflows and checklists to improve analyst productivity
- Advanced SOC functionality with threat-centric, use-case packages to deliver specific, desired outcomes (like ransomware)
- Faster time to value — 92% of customers report value in week one

To learn more about how Exabeam Fusion can help, **request a demo today**.

About Exabeam

Exabeam is a global cybersecurity leader with the mission to add actionable intelligence to every IT and security stack. The leader in next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR). Exabeam offers a comprehensive cloud-delivered solution that uses machine learning and automation focused on a prescriptive, outcomes-based approach. We design and build products to help security teams detect external threats, compromised users, and malicious adversaries while minimizing false positives to protect their organizations.

For more information, visit exabeam.com.

exabeam